Meaningful Use / HIPAA Security Risk Analysis for Medical Practices

per 45 CFR 164.308(a)(1)(ii)(A)

Bob Chaput, MA, CISSP, CHP, CHSS, MCSE
CEO and Founder
800-704-3394
bob.chaput@ClearwaterCompliance.com
Clearwater Compliance LLC
The Meaningful Use Challenge

Eligible Professionals 15 Core Objectives

1. Computerized provider order entry (CPOE)
2. E-Prescribing (eRx)
3. Report ambulatory clinical quality measures to CMS/States
4. Implement one clinical decision support rule
5. Provide patients with an electronic copy of their health information, upon request
6. Provide clinical summaries for patients for each office visit
7. Drug-drug and drug-allergy interaction checks
8. Record demographics
9. Maintain an up-to-date problem list of current and active diagnoses
10. Maintain active medication list
11. Maintain active medication allergy list
12. Record and chart changes in vital signs
13. Record smoking status for patients 13 years or older
14. Capability to exchange key clinical information among providers of care and patient-authorized entities electronically
15. Protect electronic health information

<table>
<thead>
<tr>
<th>Meaningful use Stage 1 objective</th>
<th>Meaningful use Stage 1 measure</th>
</tr>
</thead>
<tbody>
<tr>
<td>Protect electronic health information created or maintained by the certified EHR technology through the implementation of appropriate technical capabilities.</td>
<td>Conduct or review a security risk analysis per 45 CFR 164.308 (a)(1) and implement security updates as necessary and correct identified security deficiencies as part of its risk management process.</td>
</tr>
</tbody>
</table>
Regardless of the risk analysis methodology employed...

1. **Scope of the Analysis** - all ePHI that an organization creates, receives, maintains, or transmits must be included in the risk analysis. (45 C.F.R. § 164.306(a)).

2. **Data Collection** - The data on ePHI gathered using these methods must be documented. (See 45 C.F.R. §§ 164.308(a)(1)(ii)(A) and 164.316(b)(1)).

3. **Identify and Document Potential Threats and Vulnerabilities** - Organizations must identify and document reasonably anticipated threats to ePHI. (See 45 C.F.R. §§ 164.306(a)(2), 164.308(a)(1)(ii)(A) and 164.316(b)(1)(ii)).

4. **Assess Current Security Measures** - Organizations should assess and document the security measures an entity uses to safeguard ePHI. (See 45 C.F.R. §§ 164.306(b)(1), 164.308(a)(1)(ii)(A), and 164.316(b)(1)).

5. **Determine the Likelihood of Threat Occurrence** - The Security Rule requires organizations to take into account the likelihood of potential risks to ePHI. (See 45 C.F.R. § 164.306(b)(2)(iv)).

6. **Determine the Potential Impact of Threat Occurrence** - The Rule also requires consideration of the “criticality,” or impact, of potential risks to confidentiality, integrity, and availability of ePHI. (See 45 C.F.R. § 164.306(b)(2)(iv)).

7. **Determine the Level of Risk** - The level of risk could be determined, for example, by analyzing the values assigned to the likelihood of threat occurrence and resulting impact of threat occurrence. (See 45 C.F.R. §§ 164.306(a)(2), 164.308(a)(1)(ii)(A), and 164.316(b)(1)).

8. **Finalize Documentation** - The Security Rule requires the risk analysis to be documented but does not require a specific format. (See 45 C.F.R. § 164.316(b)(1)).

9. **Periodic Review and Updates to the Risk Assessment** - The risk analysis process should be ongoing. In order for an entity to update and document its security measures “as needed,” which the Rule requires, it should conduct continuous risk analysis to identify when updates are needed. (45 C.F.R. §§ 164.306(e) and 164.316(b)(2)(iii)).
I. Practice completes user-friendly web-based Clearwater Risk Analysis Smart Questionnaire™

II. Consultant facilitates phone call / web meeting follow-up to data additional and/or more specific details

III. Consultant develops and delivers HIPAA Security Risk Analysis Report

The Solution

“Remote” Meaningful Use Risk Analysis for Medical Practices™
2 Dimensions of HIPAA Security Risk Analysis

1. What is our exposure of our information assets (e.g., ePHI)?

2. What do we need to do to treat or manage risks?

A Risk Analysis Addresses Both
Sample Proposal TOC

Table of Contents – Proposal Outline

Proposal Includes Clearwater Compliance Intellectual Property ........................................... 4
1. Risk Analysis Activities ............................................................................................................. 5
2. Company Overview .................................................................................................................. 6
3. Statement of Work and Deliverables ....................................................................................... 7
4. Out of Scope Work Items ......................................................................................................... 8
5. Summary of Fees and Timeline for Initial Engagement .......................................................... 9
6. Sample Team Member Biographies ......................................................................................... 10
7. Proposal Acceptance ............................................................................................................... 12
Table of Contents
Introduction ................................................................. 3
Scope ............................................................................. 3
Methodology................................................................. 3
System Characterization ............................................... 4
Threat Identification....................................................... 5
Vulnerability Identification ............................................. 7
Control Analysis.......................................................... 8
Likelihood Determination ............................................... 12
Impact Analysis ........................................................... 13
Risk Determination ....................................................... 14
Control Recommendations ........................................... 16
Revision History ........................................................... 17

Risk Analysis Report Proves Completion!
Value Created for Medical Practices

1. Assistance with Meaningful Use Stage I Attestation ➔ Incentive $$$$$
2. Important step towards HIPAA Security compliance
3. Work with trusted partner (Clearwater Compliance LLC)
4. Access to HIPAA-HITECH experts for additional compliance progress
5. Demonstrate “good faith effort”
Value – Added Pricing Model Based on Number of Practitioners:

- Designed for Small Medical Practices with under 20 Practitioners
- Focused on / limited to assets that create, receive, maintain or transmit ePHI

<table>
<thead>
<tr>
<th>Practitioners</th>
<th>1st</th>
<th>2nd-3rd</th>
<th>4th - 10th</th>
<th>11th - 20th</th>
<th>Over 21</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>$800</td>
<td>$400</td>
<td>$200</td>
<td>$150</td>
<td>Quote</td>
</tr>
</tbody>
</table>
Choose Clearwater Compliance Today!

- Earn Meaningful Use Incentive Monies
- Enhance Revenues, Assets & Reputation
- Empower Market-facing Staff with Competitive Advantage
- Turn Compliance into Strategic Play

May We Prepare An Agreement for Us to Work Together?